Kibernetinis incidentas įvyks. Koks jūsų planas?

kpt. Mindaugas Gedminas,
NKSC prie KAM
Regioninio kibernetinės gynybos centro
Pratybų ir tyrimų skyriaus viršininkas

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Apie mane

2004 – 2013 m. administratorius / programuotojas (KAS)

2013 – 2017 m. Ryšių ir informacinių sistemų karininkas (LR atstovybė prie NATO)

2017 – 2021 m. vyr. specialistas (NKSC)

Nuo 2022 m. Pratybų ir tyrimų sk. viršininkas (NKSC)

2023-03 „ISACA Certified Information Security Manager“ sertifikacija

Turinys

- Kam reikalingas incidentų valdymo planas / procesas
- Kodėl reikia testuoti organizacijos planą / procesą
- Kuo pratybos „Kibernetinis skydas" naudingos Jūsų organizacijai

Kam reikalingas incidentų valdymo planas / procesas

Image by Arek Socha from Pixabay

Yra tik dviejų tipų įmonės: tos,

į kurias buvo įsilaužta, ir tos,

~~į kurias bus įsilaužta.~~

~~kurios nežino, kad į jas buvo įsilaužta.~~

į kurias bus įsilaužta dar kartą.

Robert Mueller, JAV FB direktorius, 2012 m.

https://en.wikipedia.org/wiki/Robert_Mueller

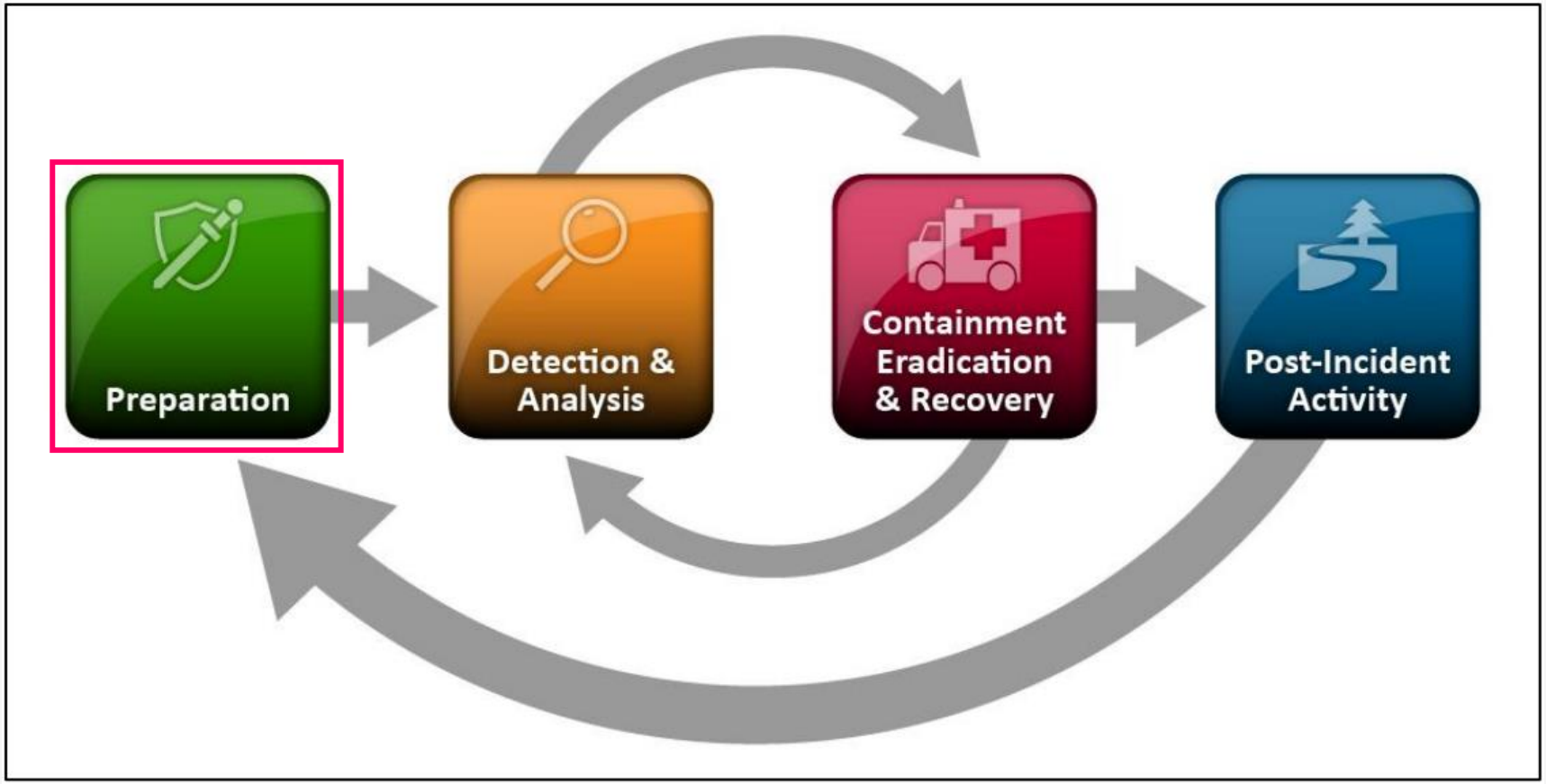
Ką daryti?

Image by PublicDomainPictures from Pixabay

Ruoštis

Image by Ryan McGuire from Pixabay

NIST incidentų valdymo procesas - pasirengimas



NIST SP 800-6: Computer Security Incident Handling Process

Tikslas – pasirengti suvaldyti incidentą.

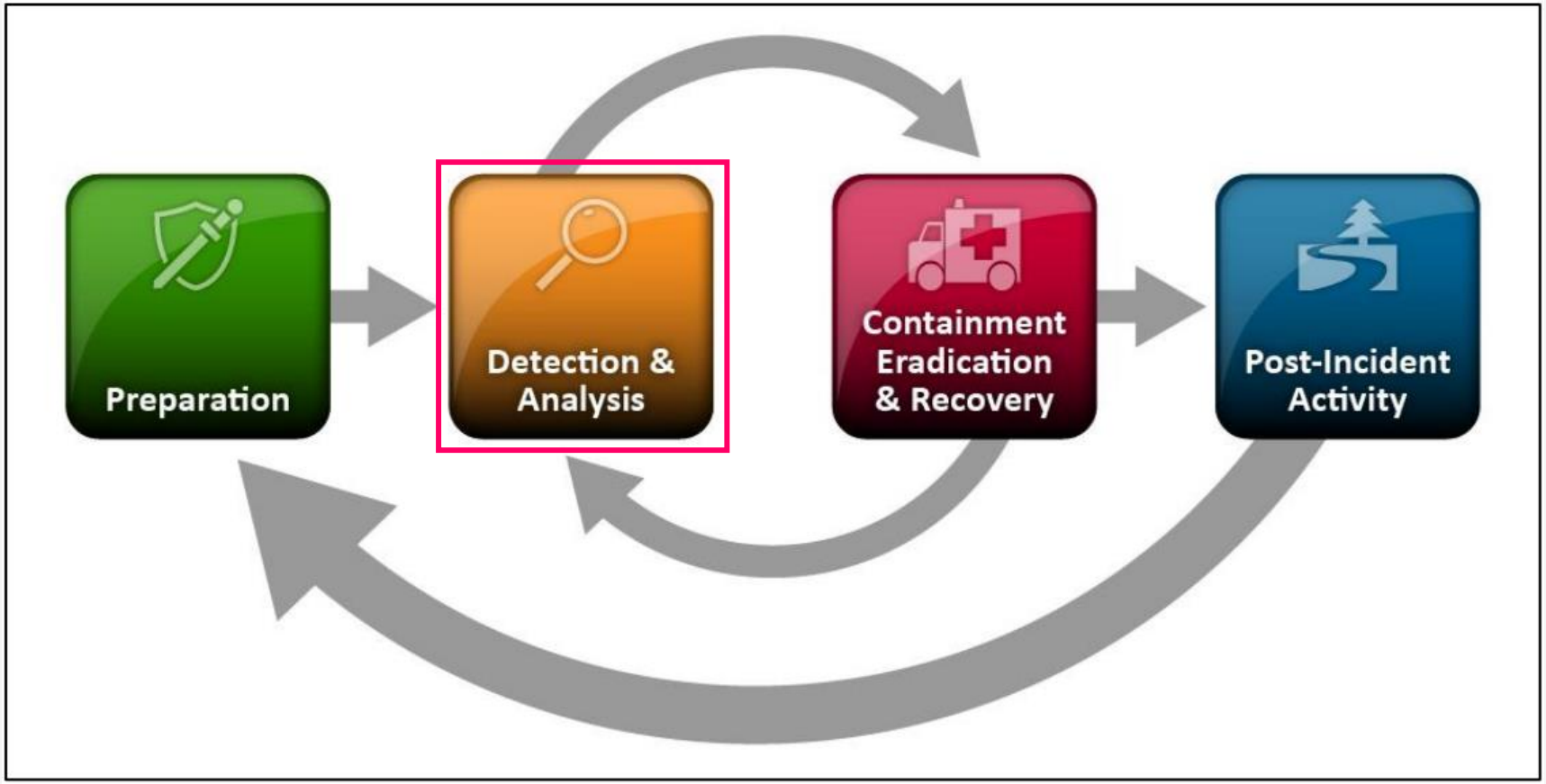
Infrastruktūros supratimas ir stebėjimas

IV proceso patvirtinimas:

- Kaip bus valdomas incidentas.
- Rolės ir atsakomybės.
- Komunikacija su sistemų savininkais ir vadovybe.
- Incidento kriterijai.
- IV komandos aktyvavimo sąlygos.

Mokymai, įrankiai, testavimas.

NIST incidentų valdymo procesas – **aptikimas ir analizė**



NIST SP 800-6: Computer Security Incident Handling Process

Tikslas – nuspręsti ar tai incidentas, jei taip - kiek kritiškas.

Pranešimo apie įvykį gavimas.

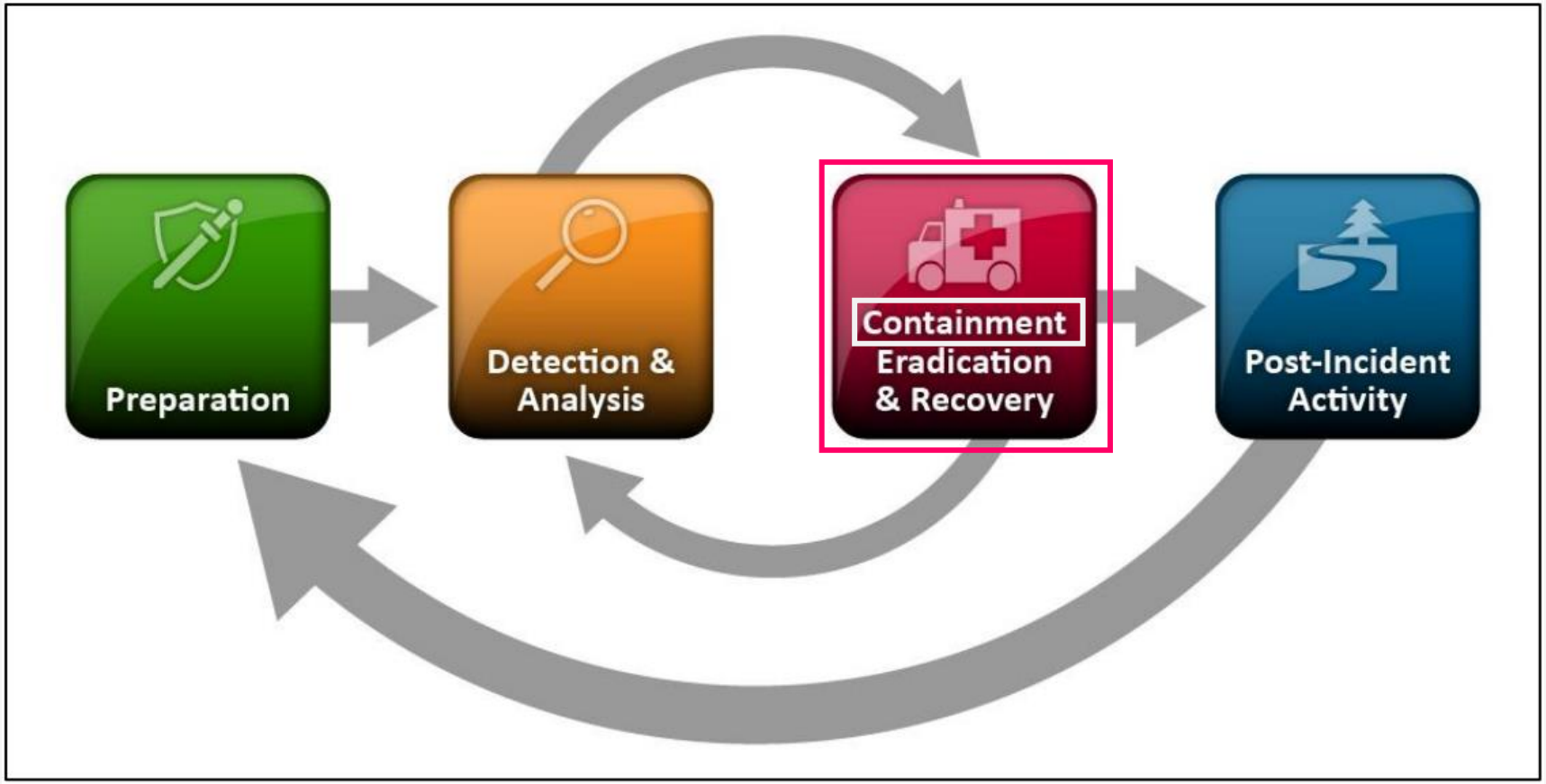
Patvirtinimas ar tai incidentas.

Nuosavybės priskyrimas.

Incidento kritiškumo nustatymas.

Eskalavimas (jei priklauso).

NIST incidentų valdymo procesas - izoliacija



NIST SP 800-6: Computer Security Incident Handling Process

Tikslas suvaldyti ir apriboti žalą.

IV komandos aktyvavimas.

Suinteresuotų šalių informavimas.

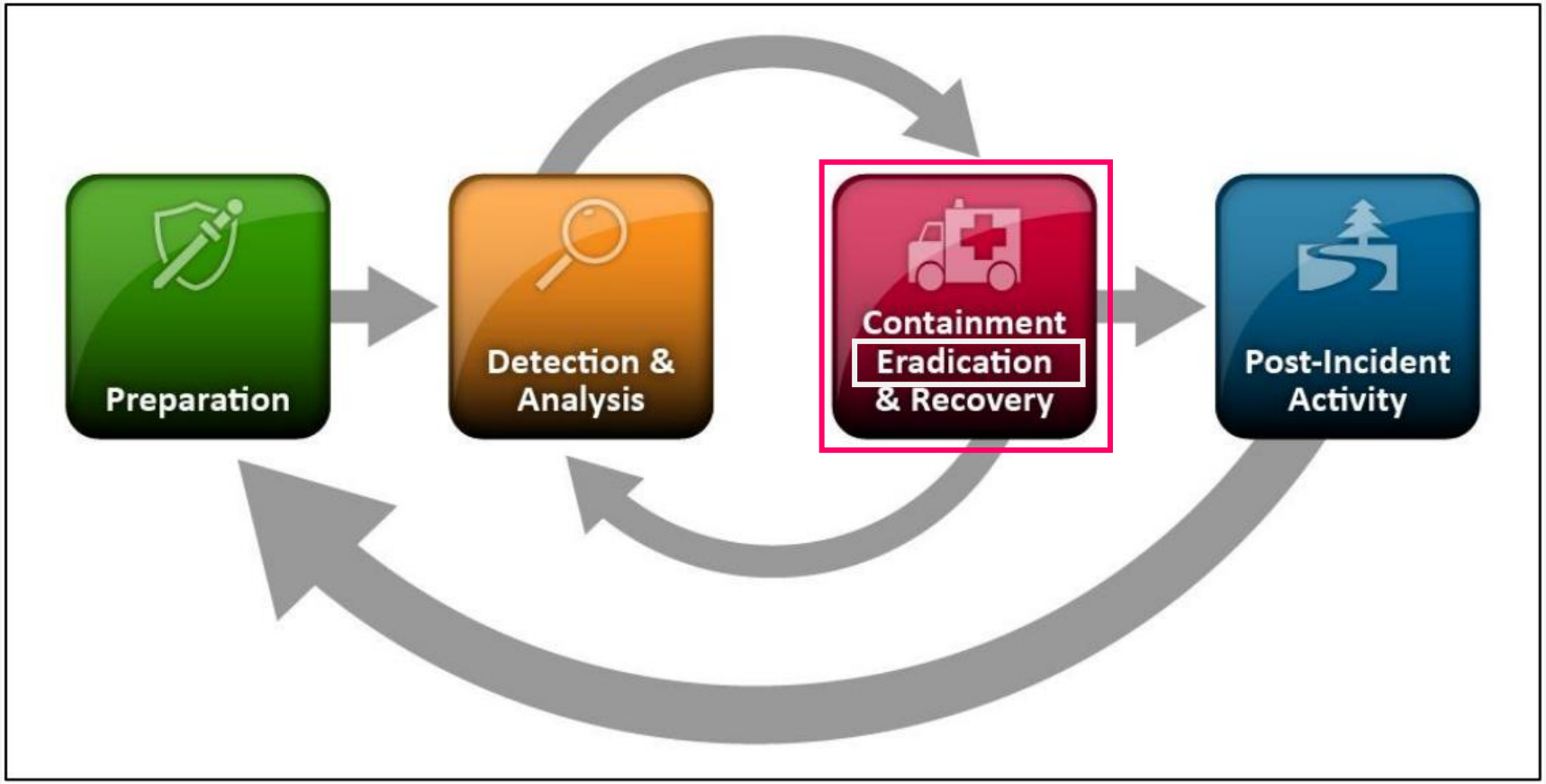
Pritarimo veiksmams gavimas.

Papildomo personalo (IT) įtraukimas.

Įrodymų išsaugojimas.

Viešoji komunikacija.

NIST incidentų valdymo procesas - išnaikinimas



NIST SP 800-6: Computer Security Incident Handling Process

Tikslas - esminės problemos radimas ir šalinimas.

Supratimas, kas lėmė incidentą.

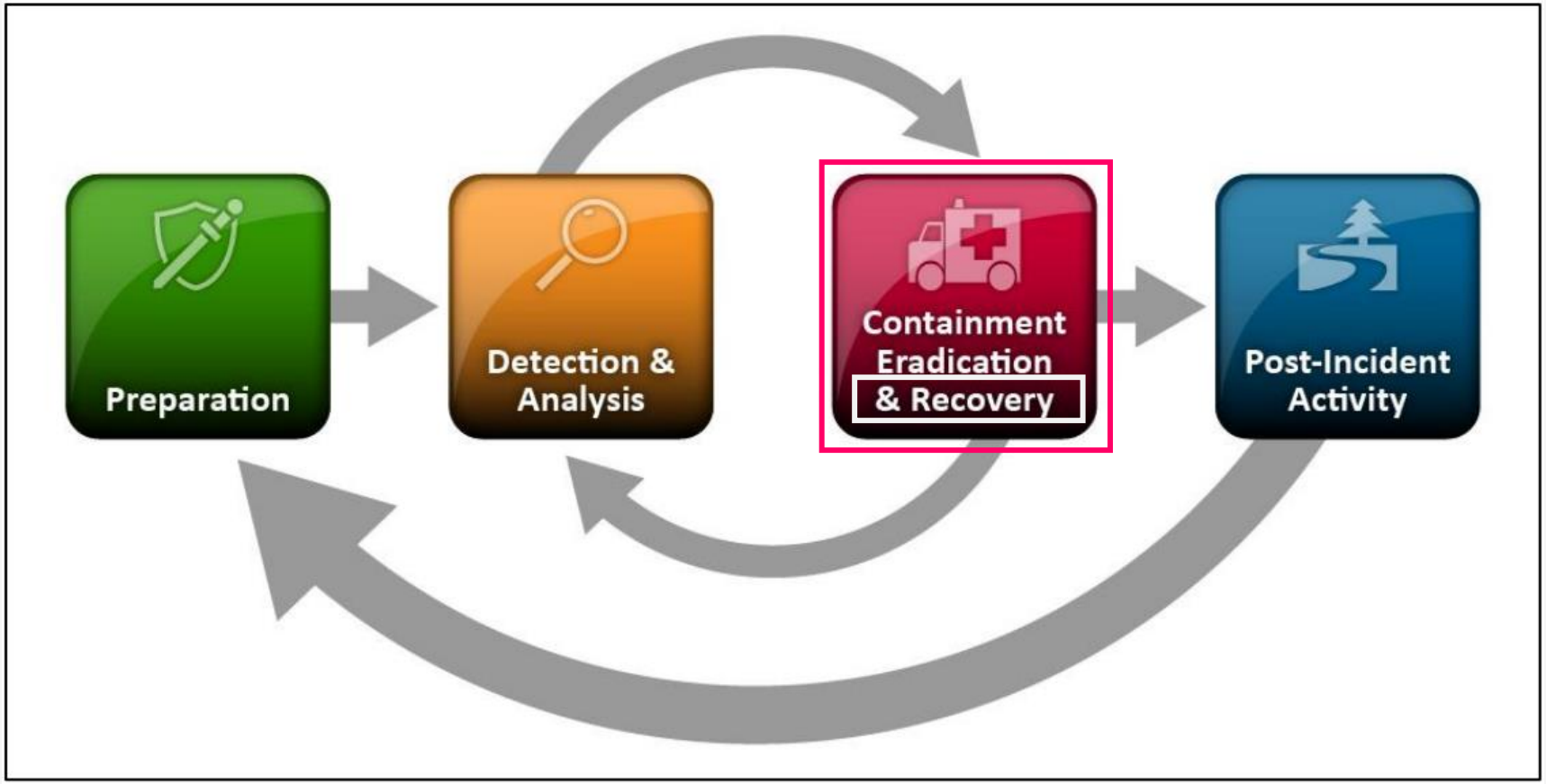
Priežasties šalinimas.

Atstatymas iš kopijos ar originalios medijos.

Gynybos stiprinimas.

Pažeidžiamumų paieška.

NIST incidentų valdymo procesas - **atstatymas**



NIST SP 800-6: Computer Security Incident Handling Process

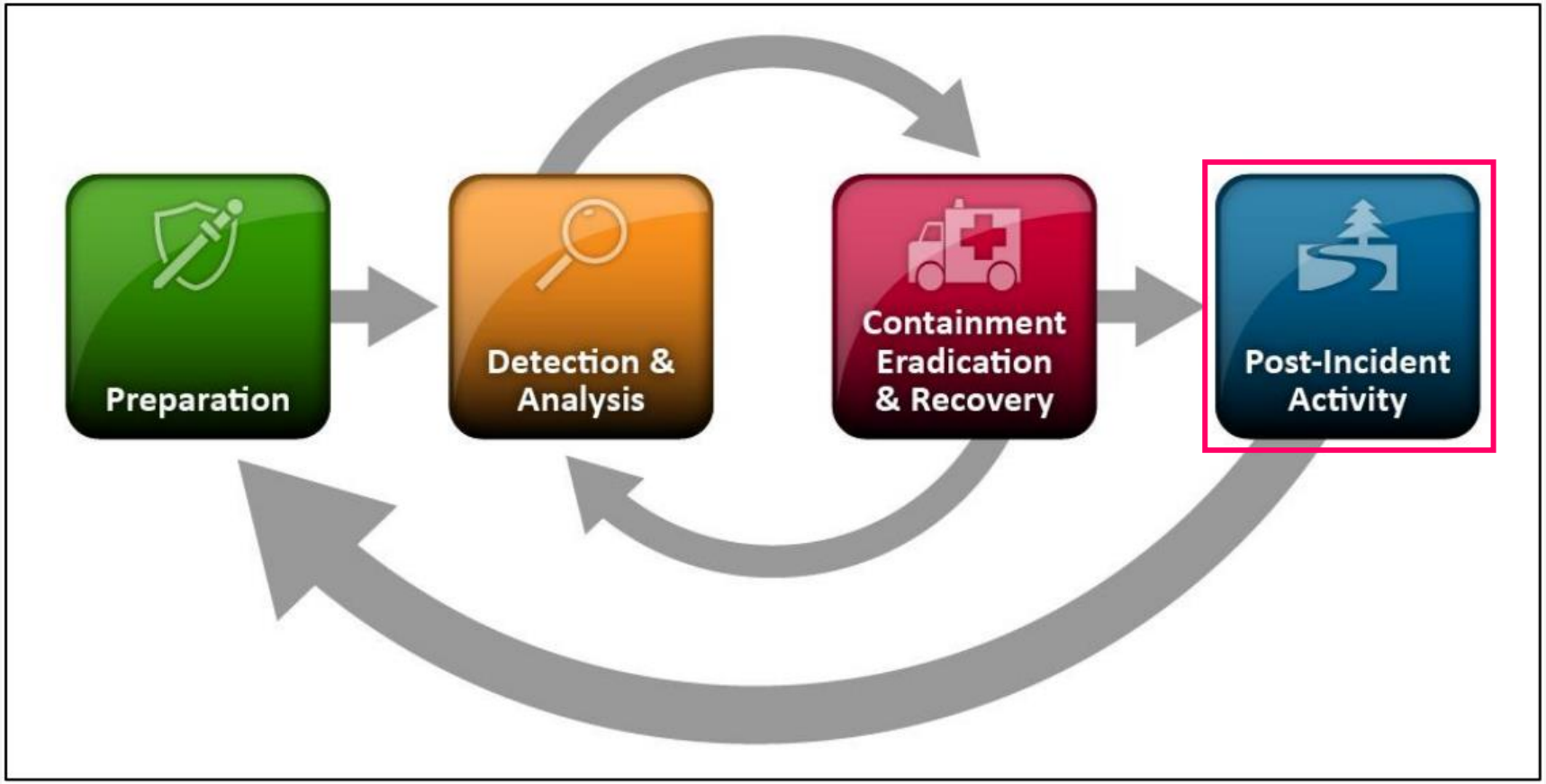
Tikslas – pilnia atstatyti paslaugas:

Patvirtinimas, kad sistemos atstatymo veiksmai buvo sėkmingi.

Sistemos savininko įtraukimas į testavimą.

Sistemos savininko patvirtinimas, kad sistema veikia tinkamai.

NIST incidentų valdymo procesas – po incidento



NIST SP 800-6: Computer Security Incident Handling Process

Tikslas – nustatyti, kas nesuveikė, ką reikia keisti.

Išsamios ataskaitos apie incidentą parengimas.

Atsako į incidentą metu iškilusių problemų analizė.

Pasiūlymai, kaip tobulinti informacijos apsaugą ir atsaką į incidentus.

Ataskaitos pristatymas suinteresuotoms šalims.

Kam reikalingas incidentų valdymo planas / procesas

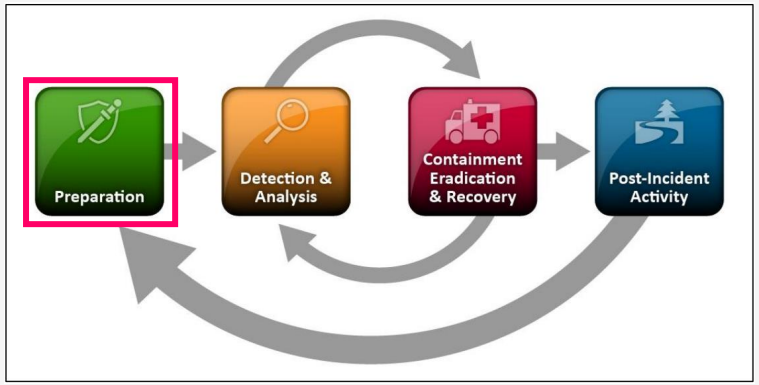


Image by Gerd Altmann from Pixabay

Kodėl reikia testuoti incidentų valdymo planą

Helmutas fon Moltkė (vyresn.),
1871-1888 m. Prūsijos kariuomenės štabo viršininkas
https://en.wikipedia.org/wiki/Helmuth_von_Moltke_the_Elder

Nė vienas planas neatlaiko pirmojo susidūrimo su priešu.

Kodėl reikia testuoti incidentų valdymo planą




Mikhail Nilov: https://www.pexels.com/photo/man-and-woman-rescuing-a-person-8942627/
Gedimino štabo bataliono nuotrauka. https://kariuomene.lt/kas-mes-esame/naujienos/buriu-vertinamosios-lauko-taktikos-pratybos-per-asmenini-meistriskuma-komandos-sekmes-link/23921#images-1
https://upload.wikimedia.org/wikipedia/commons/8/8a/Fire_drill.jpg
Sulivan Karen, USFWS on Pixnio

Kodėl reikia testuoti incidentų valdymo planą

Pratybos padeda patikrinti prielaidas

https://www.littlebobbycomic.com/projects/week-230/

Pratybų lygmenys

Pratybų lygmenys

- Strateginis
- Operacinis
- Techninis
- Naudotojų ugdymas

Kibernetinis skydas 2023

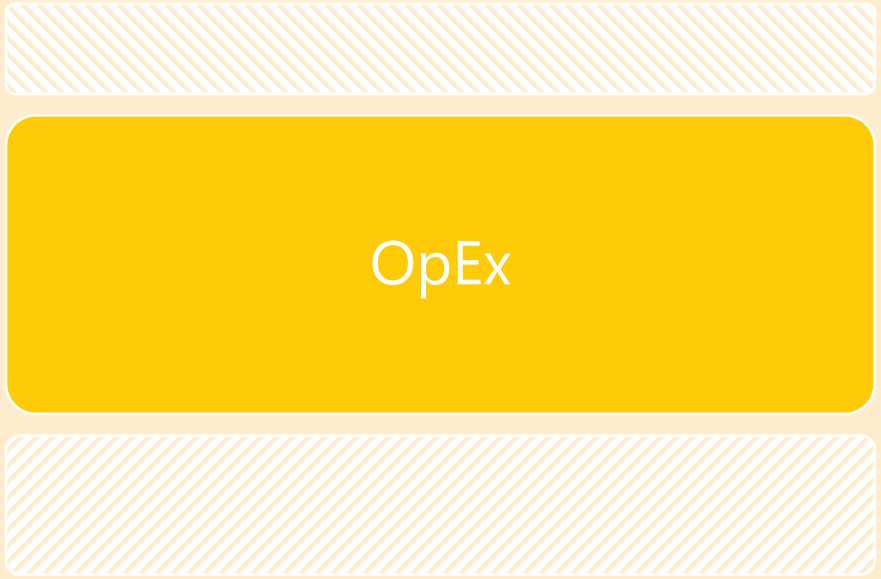
- StratEx
- OpEx
- PhishEx

Pratybų tipai

Pratybų tipai

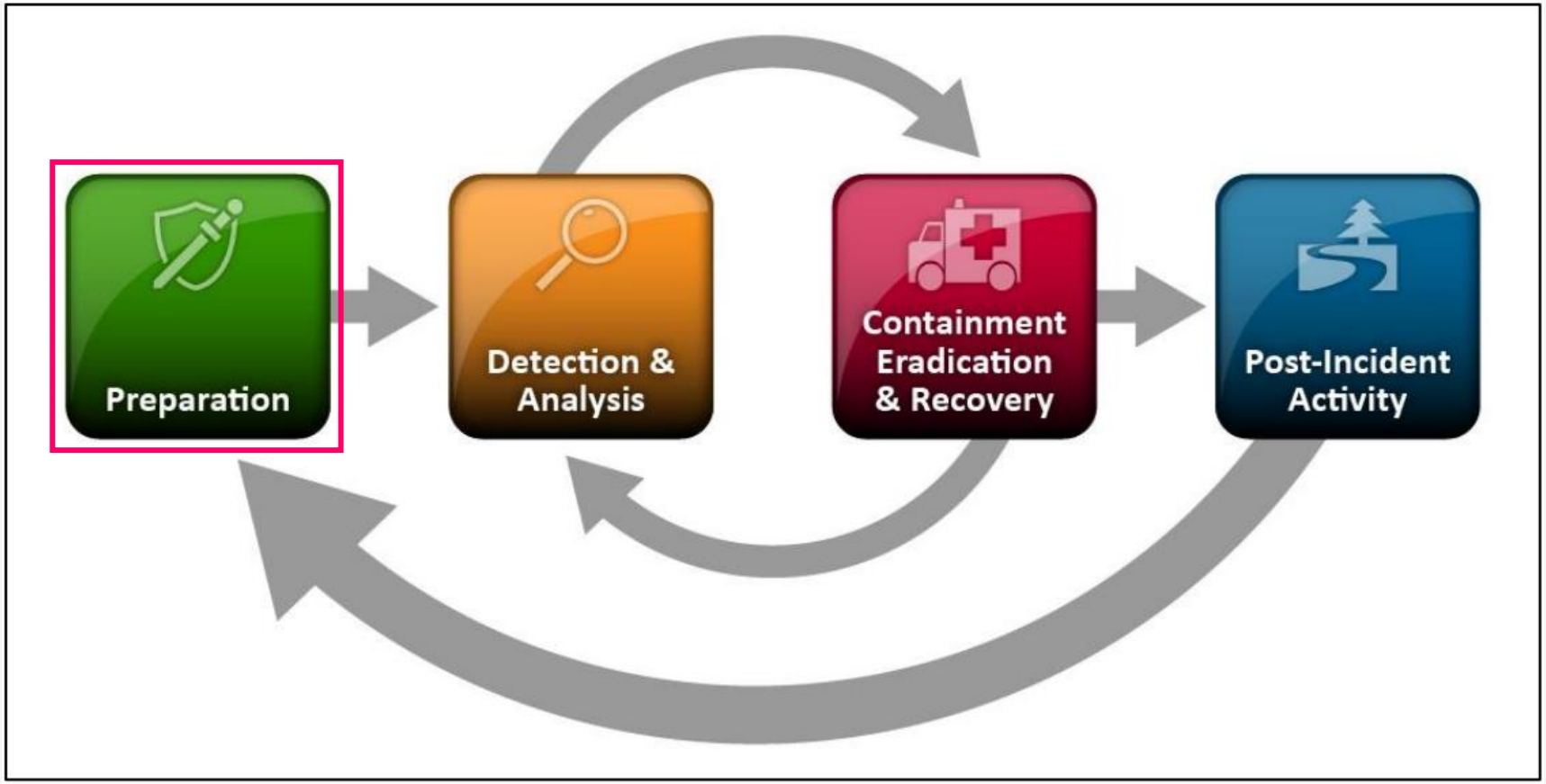
- Read-Walk-Through
- Structured Walk-Through (TTX)
- Simulation
- Parallel Test
- Full Interuption

Kibernetinis skydas 2023



Kuo Jums naudingos pratybos „Kibernetinis skydas OpEx 2023"

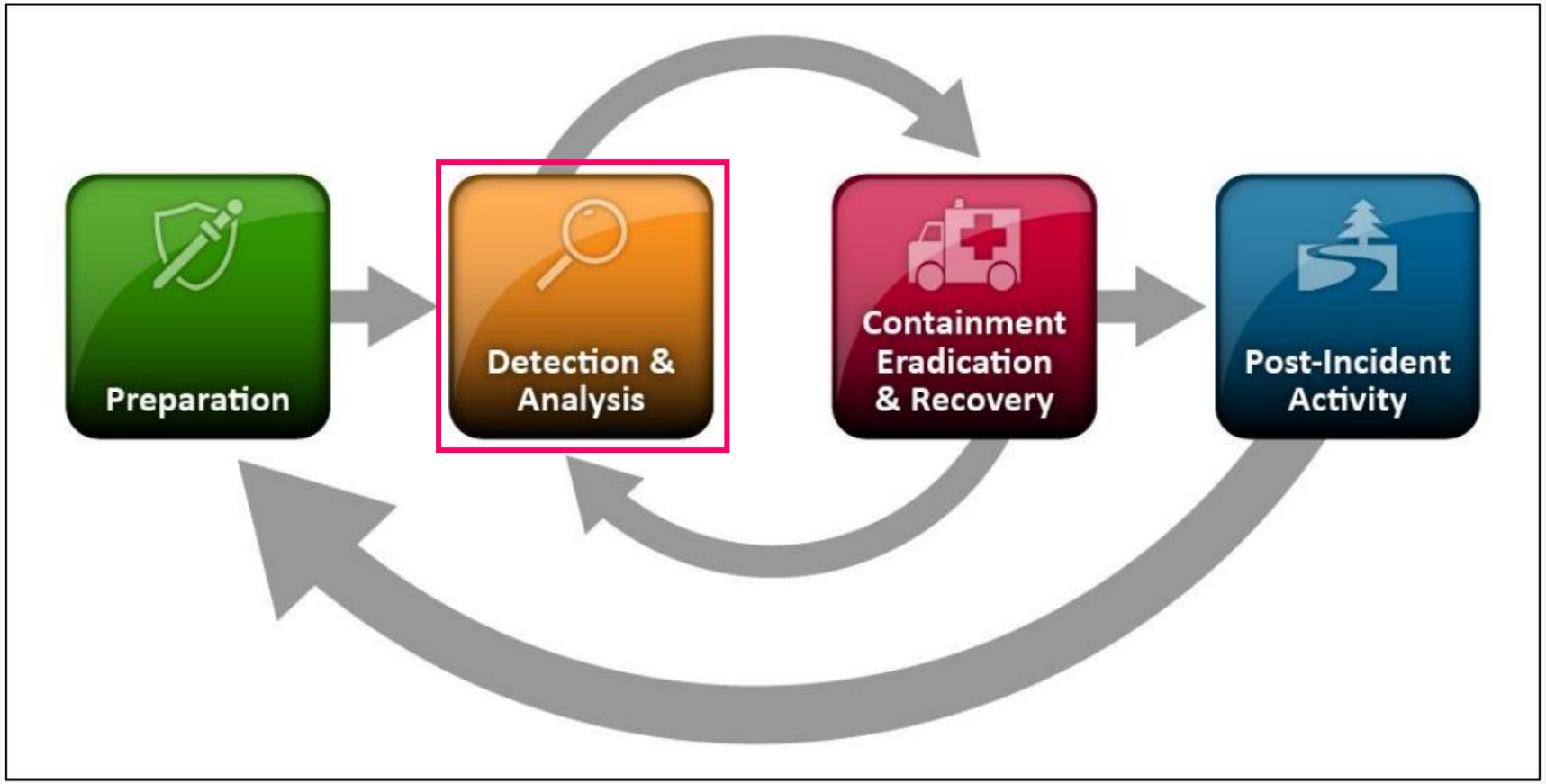
Kaip pratybos KS2023 padeda Jums testuoti savo planą / procesą



NIST SP 800-6: Computer Security Incident Handling Process

Peržiūrite, įvertinate turimą IVP arba pasirengiate IVP.

Kaip pratybos KS2023 padeda Jums testuoti savo planą / procesą



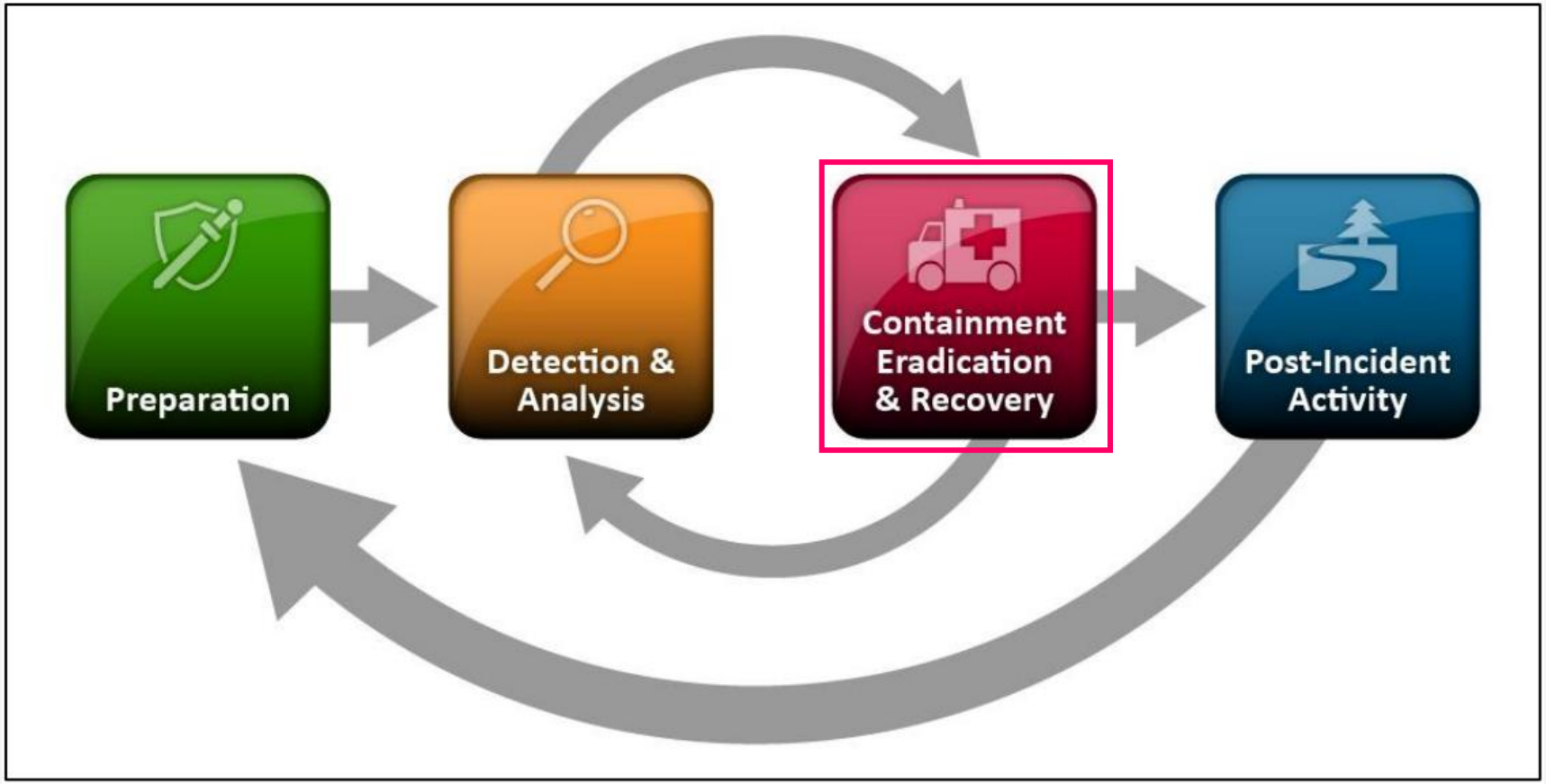
NIST SP 800-6: Computer Security Incident Handling Process

Organizacija vertina incidentą, suteikia jam kategoriją, komunikuoja.

Ugdomi techniniai įgūdžiai.

Ugdomi naudotojų gebėjimai per fišingo simuliaciją.

Kaip pratybos KS2023 padeda Jums testuoti savo planą / procesą



NIST SP 800-6: Computer Security Incident Handling Process

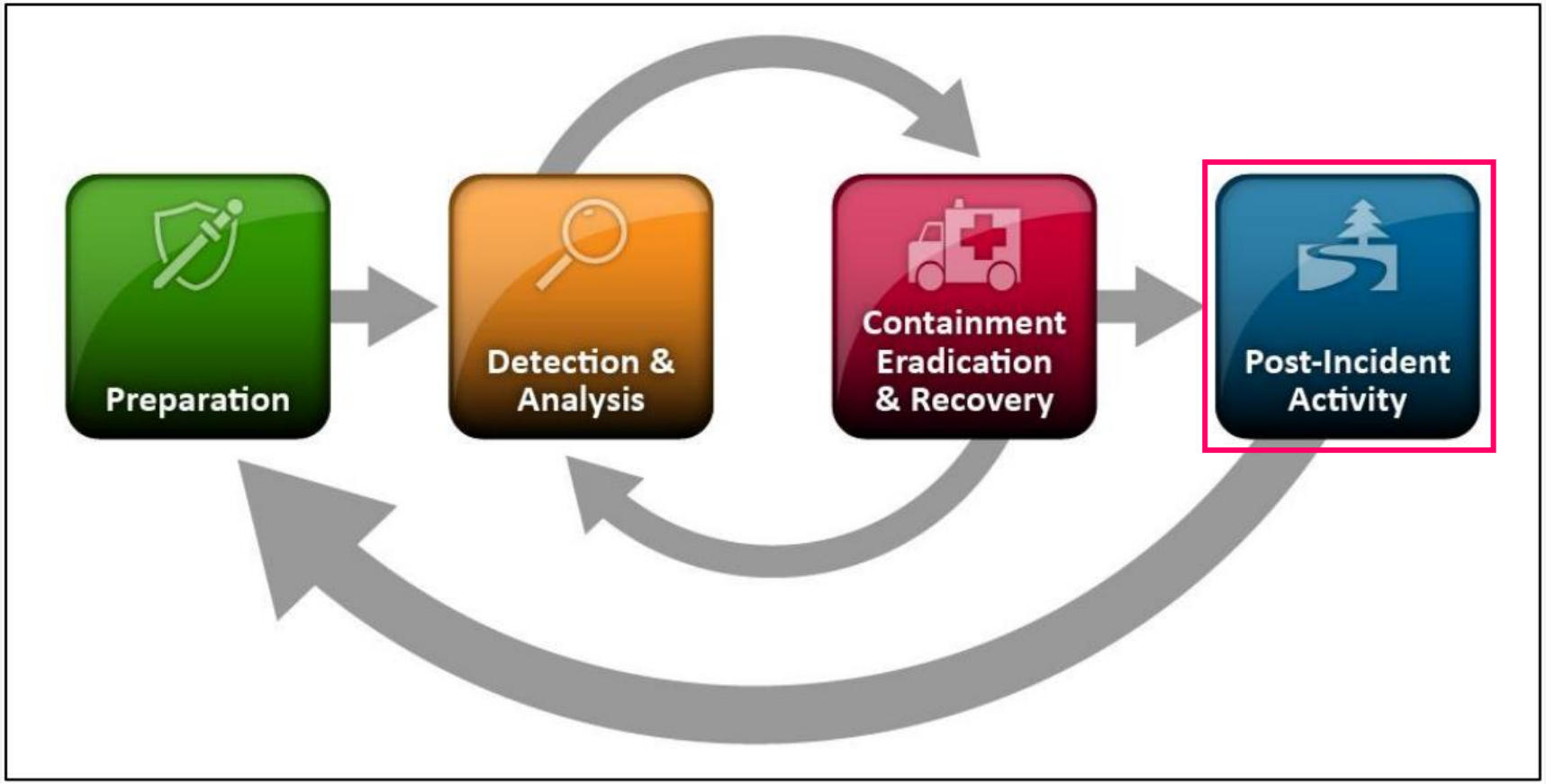
Organizacija sprendžia kaip izoliuoti, išvalyti ir atstatyti paslaugas.

Techniniai įgūdžiai.

Komunikacija su savininku ir vadovybe.

Atsarginės kopijos atstatymas.

Kaip pratybos KS2023 padeda Jums testuoti savo planą / procesą



NIST SP 800-6: Computer Security Incident Handling Process

Veiksmų vertinimas.

Identifikuotos pamokos, trūkumai.

IVP tikslinimas.

Ataskaita vadovybei.

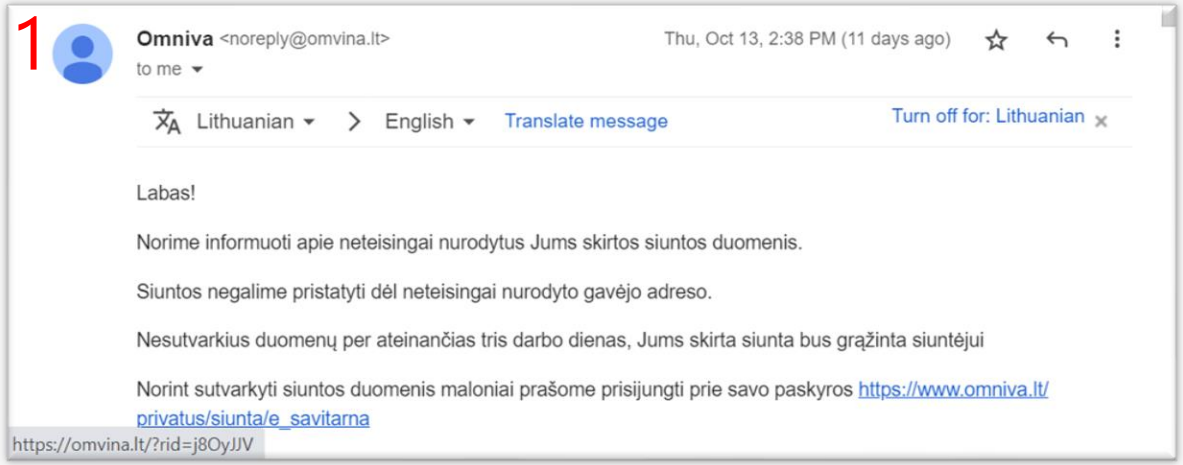
Kuo Jums naudingos pratybos „Kibernetinis skydas PhishEx 2023“

Įrankis personalo atsparumo fišingui patikrinti – **Gophish;**

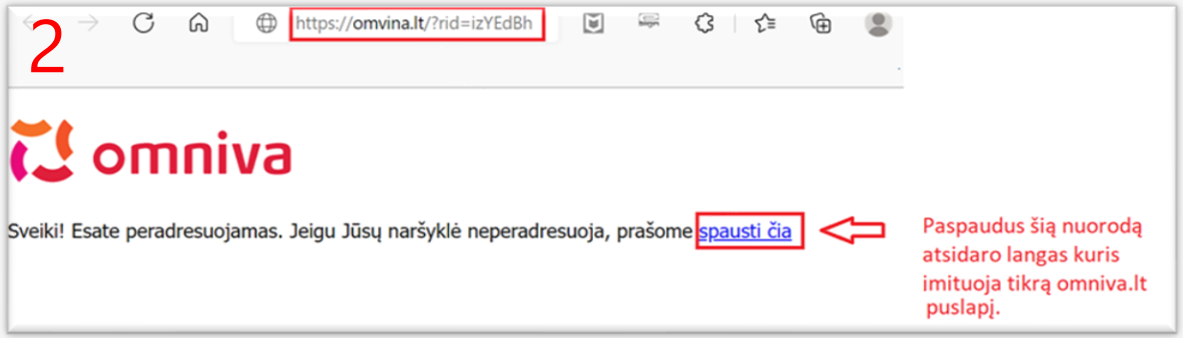
- El. laiškai ir tinklalapiai, imituojantys žinomas paslaugas;
- Domenai, panašūs į žinomus (omvina.lt, KVTC ir kt.);
- Paprasta dalyvauti, lengva kalbėtis apie kibernetinį saugumą su darbuotojais.

KS2022 fišingo simuliacijos rezultatai

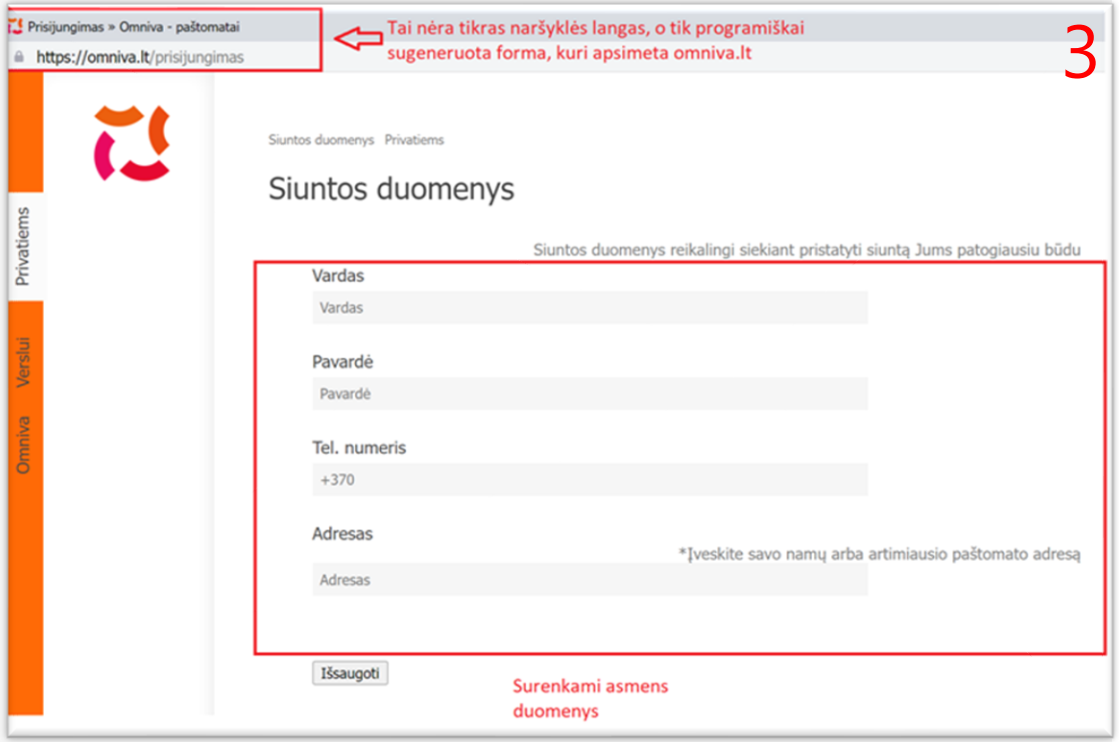
1



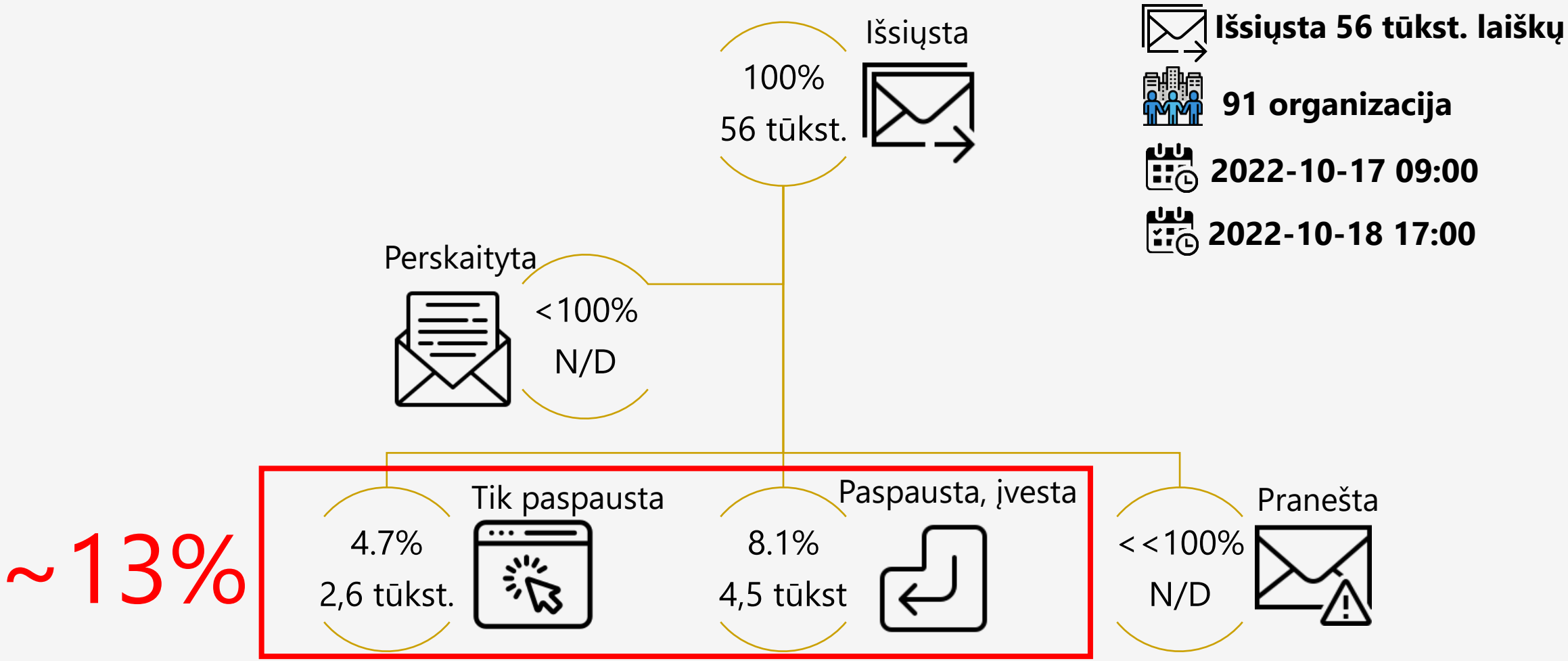
2



3



KS2022 fišingo simuliacijos rezultatai



Tolimesni žingsniai

Įvadinė konferencija – balandžio 6 d.

Organizacijos sprendimas – atstovas planavimui.

Kibernetinis skydas OpEx - spalio 17-19 d.

Kibernetinis skydas PhishEx – nuolat 2023 m..

Rekomendacijos

Jeigu nedalyvavote anksčiau - prisijunkite į Kibernetinis skydas OpEx.

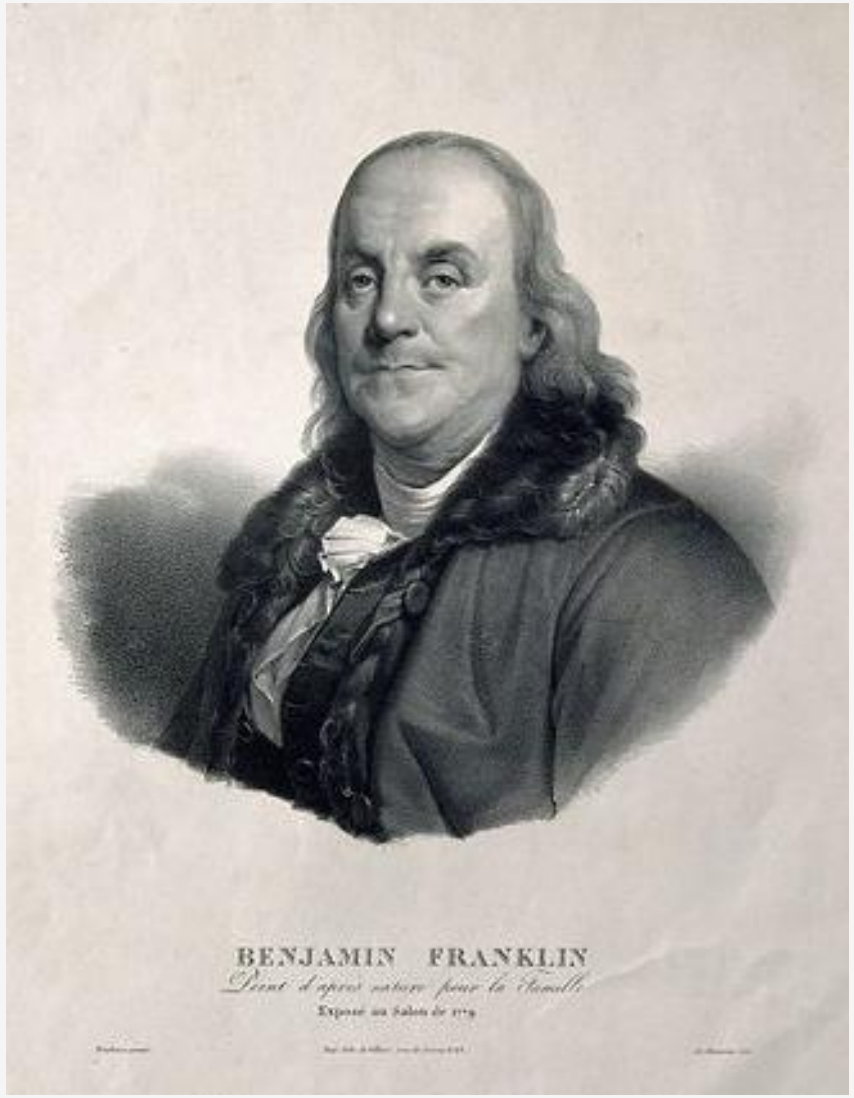
Jeigu nedrąsu dėl vadovybės įsitraukimo – apsiribokite IT / KS personalu.

Jeigu galite - įtraukite ir vadovus, bei kitas suinteresuotas šalis.

Jeigu jau pernai buvote įtraukę – didinkite ambicijas, spaudimą.

Jeigu nežinote nuo ko pradėti, tai pradėkite nuo Kibernetinis skydas Phishex 2023.

Jei nesiruošiate, ruošiatės nesėkmei.



Pabaigai

From: [redacted]
Sent: [redacted] December 2022 [redacted]
To: KAM Nacionalinis kibernetinio saugumo centras
Subject: del [redacted] svetainės

Sveiki,

Šiandien gavome pranešimą iš Interneto vizijos, kurioje talpinama [redacted] svetainė [redacted]

Pažeidimai

Pagal sutartyje numatytas paslaugų teikimo sąlygas užsakovas įsipareigoja užtikrinti, kad jam suteiktos paslaugos nebus naudojamos neteisėtais tikslais, įskaitant, bet neapsiribojant masiniu el. pašto siuntimu, kenkimu kompiuterinių sistemų, tinklų veikimui ar saugumui, taip pat pažeidžiant galiojančius Lietuvos Respublikos teisės aktus, Vykdytojo bei trečiųjų asmenų teises.
Žemiau yra užfiksuoti Jūsų paslaugų sutarčių pažeidimo atvejai. Paspauskite ant pažeidimo norėdami pamatyti išsamesnę informaciją ir pranešti apie pažeidimo pašalinimą.

Nepranešus apie pažeidimo pašalinimą iki nurodyto termino, paslaugos veikimas bus automatiškai anuliuotas.

Pažeidimas	Paslauga	Terminas	Atsakyta	Uždaryta	Vertinimas
[redacted]	Svetainės talpinimas ir el. paštas (planas Svetainei, [redacted]	Gruodžio [redacted] 2022 [redacted]	Gruodžio [redacted] 2022 [redacted]		

Papildoma informacija: https://www.ivi.lt/pagalba/Sutarties_sąlygų_pažeidimai

« Grįžti į pradžią

Gal galite padėti, ką mums reikėtų daryti? Ačiū!

[redacted]
[redacted]
Viešųjų ryšių specialistė
[redacted]

Klausimai

Image by Gerd Altmann from Pixabay

Bendraukime

mindaugas.gedminas@nksc.lt

www.linkedin.com/in/mindaugas-gedminas